PBMA-SSL
Secure Work Groups

New User Authentication And Activation Plan (NUAAP)

Prepared for the
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
Report No. 0190602.12.004
Revision 1

April 15, 2004

ARES CORPORATION
21000 Brookpark Road
MS 501-4
Cleveland, OH 44135

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

The Process Based Mission Assurance (PBMA) Secure Socket Layer (PBMA-SSL) application is designed to provide users with secure collaborative work groups ("Work Groups") using a validated method of strong user authentication. The PBMA-SSL application enables the sharing of information deemed as sensitive/critical data such as Source Evaluation Board (SEB) data, and information governed under the International Traffic Arms Regulated (ITAR) or Export Administration Regulations (EAR) laws. The PBMA-SSL application operates behind the NASA Glenn Research Center (GRC) firewall. The Work Groups are designed to organize information, manage documents, share schedules and facilitate efficient project team collaboration, all in a browser-based environment.

1.2 Roles

1.2.1 PBMA Secure Work Group Originator

The Work Group Originator ("Originator") is the initial Work Group Administrator ("Administrator"). The Originator is the data owner who approves any data that will reside in the Work Group. The Originator may not want to administer the Work Group and may assign other members of the Work Group to fill that role. The Originator will be the conduit for all password resets (reference Section 4).

As the data owner, the Originator assumes responsibility for all information posted to the Work Group.

If the Work Group will contain ITAR/EAR or any other ACI information, the Originator must fill out Appendix A – National Agency Check Verification. The Originator is also responsible for verifying their Member's ability to access ACI data (keeping in-line with Code I requirements).

Reference NPR 2190.1 for NASA's current ITAR/EAR policy.

Note: No ACI data shall not be accessed from a user's home PC.

1.2.2 PBMA Secure Work Group Administrators

Work Group Administrators are responsible for the maintenance of the Work Group site. This maintenance includes performing all administrative functions such as managing Work Group membership and access, updating general information, and review of

information, content, and site activities to ensure compliance to NASA policies and the PBMA-SSL Charter. Even if the Originator maintains control over the administration of the Work Group, a back up Administrator is prudent.

While the Work Group Administrator can perform membership and access functions, only the Originator can perform these functions for Work Groups containing ACI data.

1.2.3 PBMA Secure Work Group Members

The Work Group Members ("Members") are the end-users of the Work Group site.

1.2.4 PBMA Secure Work Group Technical Support

Work Group Technical Support ("Technical Support") is comprised of PBMA-SSL Information Technology (IT) personnel who are responsible for maintaining the backbone of the PBMA network, the Web site application, and the PBMA-SSL Help Desk ("Help Desk") which is the primary interface between of the PBMA-SSL IT personnel and Administrators. Technical Support may also include other application support personnel when needed.

2 SECURITY PRACTICES

All Work Group Originators, Administrators, Members and Technical Support personnel must take responsibility for protecting Administratively Controlled Information (ACI). ACI information must be safeguarded by protecting login information to protect access to ACI information stored in a Work Group, configuration of a Work Group, monitoring membership of the Work Group and information stored in a Work Group, and possession and handling of ACI information.

2.1 Administratively Controlled Information

Administratively Controlled Information is official information and material, of a sensitive but unclassified nature, which does not contain national security information (and therefore cannot be classified), nonetheless, should still be protected against inappropriate disclosure. Within NASA, such information may have previously been designated "FOR OFFICIAL USE ONLY." This NASA designation has been changed to "Administratively Controlled Information," for clarity and to more accurately describe the status of information to be protected. Information that falls in this category includes:

- ITAR: International Traffic in Arms Regulations
- EAR: Export Administration Regulations
- MCTL: Military Critical Technologies List
- FAR: Federal Acquisition Regulations
- FOIA: Freedom of Information Act and the Privacy Act of 1996
- UCNI: Unclassified Controlled Nuclear Information.

2.2 Protecting Login Information

Work Group accounts are established in a manner that ensures access is granted on a need to know and least privilege basis. Work Groups rely on a combination of user name, which establishes the identity of the user for the computer or system, and a password, which is known only to the authorized user and authenticates that the user is who he or she claims to be. Passwords are simpler and cheaper than other, more secure forms of authentication such as special key cards, fingerprint ID machines, and retinal scanners. They provide a simple, direct means of protecting a system or account. Being simpler and cheaper, they require greater attention by the user to protect.

- Never transmit user name or password by e-mail, fax, instant messaging, pager, or other electronic means. *User name and password will always be provided verbally, once the user's secret question has been correctly answered.*
- Never record login information in an unprotected location - electronic or physical, where unauthorized individuals can access it.
- Passwords must be a minimum of eight characters. The eight characters will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters.
- Passwords must be changed every 90 days.

2.3 Work Group Configuration

In support of these security standards, certain functions have been disabled in the PBMA-SSL application. They include, but are not limited to:

- The Live Chat functionality
- Community Messenger (Instant messaging tool)
- The option of selecting the "Remember me" function on the login page.

Originators will be given Founder status within the PBMA-SSL application. Founder status is generally given to the founding member of the work group. There can only be one founder at any time. The founder has complete control over all content and community administration. They have the ability to delete any user's membership. The founder status can be passed to another member of the community - this can only be done by the founder. Also, this status permits modification of Work Group specific security settings. The Founder must take extreme care in enforcing baseline requirements:

- Under Administration → Community Security, do not alter these settings. The default settings should not be altered from their current configuration.
    - Work Groups that contain ITAR/EAR or other ACI data shall always be "Private," i.e., new Members must be invited and approved by the Founder or an Administrator in order to join the group. The Originator must maintain complete control of membership functions in Work Groups containing ACI data.
    - All other Work Groups shall be "Restricted," i.e., new Members can be invited by a current Member, or approved for membership by an Administrator.
    - In rare instances a Work Group may be "Open" by special request only.

2.4 Work Group Monitoring

2.4.1 Membership

Administrators are responsible for ensuring that membership is limited to individuals with a legitimate need to access their Work Group. However, final membership authority will always reside with the Originator. Good security practices include:

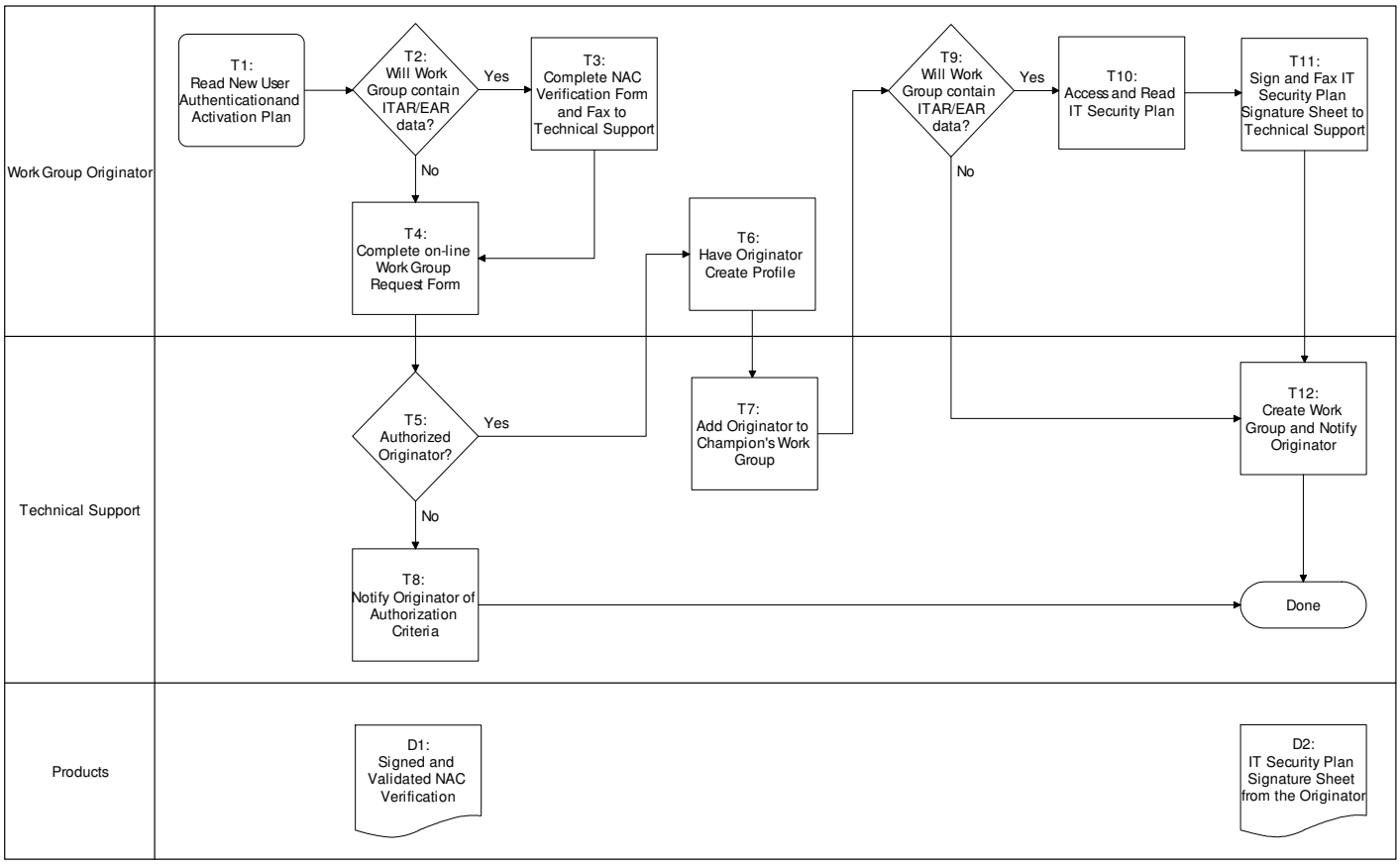
- Verifying who is requesting membership and their need for such membership.
- Removing Inactive Users. Note: If the member to be removed has been designated as an Administrator, Technical Support must be notified to complete the removal process.
- Deleting members who no longer require or are no longer involved in the process or activity supported by the Work Group.
- Request site deactivation at conclusion of Work Group activity.

2.4.2 Information

The Originator should review material in each of their Work Groups for possible designation as ACI prior to use. Criteria of at least one of the following must be met to qualify as ACI:

- Information Protected by Statute: Export Administration Act; Arms Export Control Act; Space Act (Section 303b)
- Information the originator determines to be unusually sensitive or critical to the success of the program or project.
- Information Exempt from Freedom of Information Act (FOIA); which includes:
    - Internal Personnel Rules/Practices
    - Trade Secrets/Commercial/Financial
    - Inter/Intra-Agency Memos and Letters
    - Personnel and Medical Files
    - Investigative Records
    - Financial Institution Information
    - Geological/Geophysical
    - Maps/Documents of underground utilities
    - Drawings/specifications for Mission Essential Infrastructure (MEI) or other assets
    - Mission specific security plans
    - Emergency Contingency plans

3 PROCESS FOR ACTIVATING A NEW WORK GROUP



TASKS

T1. *Read the NUAAP, which contains the Secure Work Groups (PBMA-SSL) General Charter:* The Originator reads the NUAAP to become familiar with the purpose of the Work Groups and the responsibilities associated with them.

T2. *Determine if Work Group will contain ITAR/EAR or other ACI data.*

T3. *Complete NAC Verification form and Fax to Technical Support:* If the Work Group will contain ITAR/EAR or other ACI data, the Originator will fax the completed NAC verification form (0) to Technical Support at 1-216-433-2701.

T4. *Complete on-line Work Group Request Form:* Request a new Secure Work Group through the PBMA-KMS Web site (http://pbma.hq.nasa.gov/swg/).

T5. *Confirm Originator's Authorization?:* Determine if the Originator is authorized to request a new Secure Work Group.

T6. *Have Originator Create Profile.*

T7. *Add Originator to Champion's Work Group.*

T8. *Inform Originator of Authorization Criteria:* If the Originator is not authorized to direct the activation of a new Work Group, explain who is and suggest they attempt to find a sponsor within that group.

T9. *Determine if Work Group will contain ITAR/EAR or other ACI data.*

T10. *Access and Read the PBMA-SSL IT Security Plan (Report No. 0190602.12.007):* If the Work Group will contain ACI data, once the Originator logs into the Champion's Work Group, the Originator must access and read the IT Security Plan.
T11. *Sign and Fax IT Security Plan Signature Sheet:* If the Work Group will contain ITAR/EAR or other ACI data, the Originator, as the prospective Work Group Data Owner, indicates acceptance of the plan by signing the plan's concurrence sheet.
T12. *Create Work Group and Notify Originator:* Originator will be notified by Technical Support once their Work Group is created. The system utilizes single sign-on (SSO) so all subsequent groups will use the same user ID and password.

DELIVERABLES

D1. *Signed and Validated NAC Verification.*
D2. *IT Security Plan Signature Sheet from Originator.*

3.1 Read Secure Work Group NUAAP

The NUAAP contains the Work Group Charter, basic rules and procedures.

Note: PBMA-SSL Program Management reserves the right to deny requests for activation of any Work Group, or to delete any existing Work Group, that does not comply with the intent of the Secure Work Groups (PBMA-SSL) General Charter.

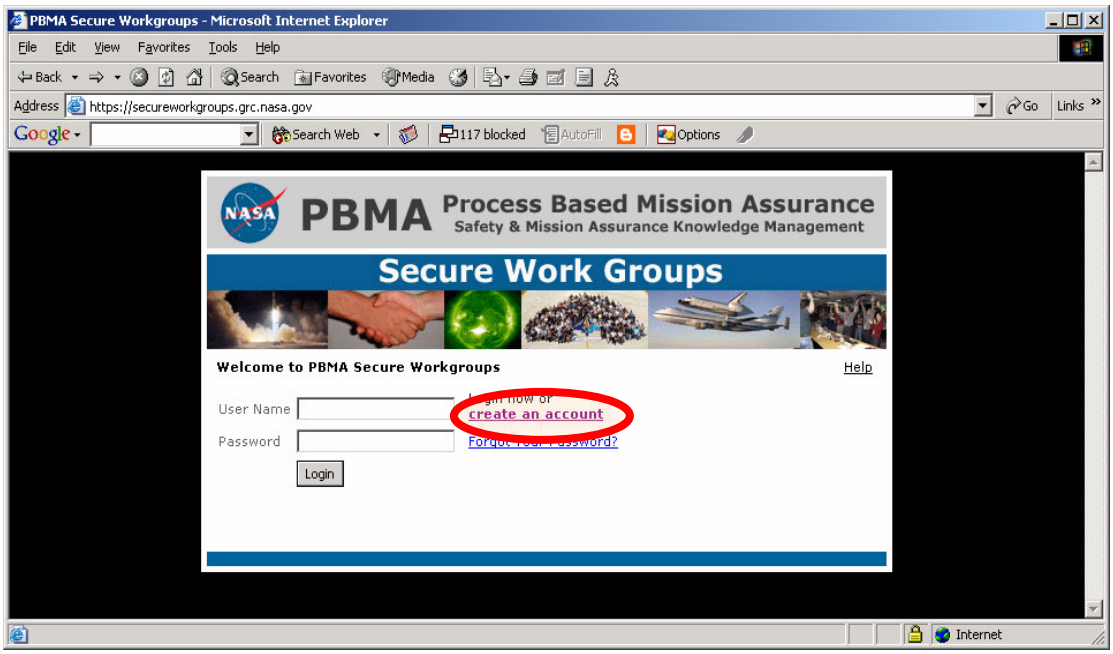
3.2 Approvals Required

Work Groups are available to all NASA and contractor personnel, industry partners and academia. All Originators are required to submit proof of United States citizenship via the NAC Verification Form (see 0).

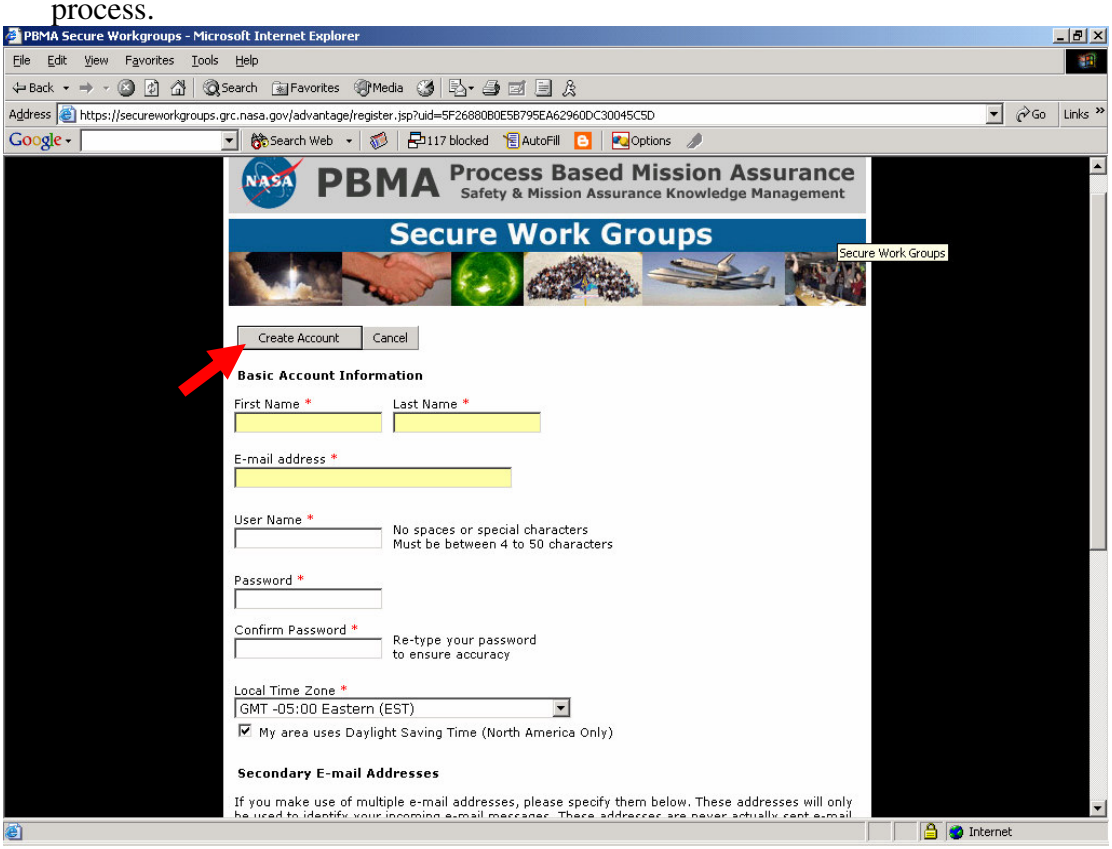
3.3 Creating a Secure Work Group Account

Once the Originator meets the criteria for obtaining a Work Group, the Originator must create their account. Once the account is created, the Originator's account will then be added to the Champion's Work Group. The Champion's Work Group is for Originators only and will have information that pertains only to Originators. The user name and password created by the Originator in this process will be universal for all Work Groups in which the Originator will have membership. This application takes advantage of single sign-on (SSO). The following is a step-by-step instruction on how the Originator is to create their account:

a. Go to https://secureworkgroups.grc.nasa.gov/
b. Click the "create an account" link.



c. Fill out the on-line form and click the "Create Account" button to complete the process.



3.4 Accessing the PBMA-SSL IT Security Plan

Once an Originator is approved and they have created their account, they will be added to the Champion's Work Group and made a member of the "Sensitive Information Work Group" which will allow the Originator access to the *PBMA-SSL IT Security Plan* ("IT Security Plan"). The Champion's Work Group is for Originators only and will have information that pertains only to Originators.

Note: Users of the Secure Work Groups will only have one account. One user ID and one password will be used for access to all Secure Work Group.

Once the Originator accesses and reads the IT Security Plan, they must sign the signature sheet, Appendix C of the *PBMA-SSL IT Security Plan*. By signing this plan, the Originator gives consent as the Data Owner for their sensitive information to reside on the Work Group. The signature sheet, with the Originator's original signature, must be provided to Technical Support. In order to expedite the activation process, a facsimile is recommended. The Work Group cannot be activated without the Originator's signature on the PBMA-SSL IT Security Plan.

3.5 Work Group Request

Note: The Originator is responsible for the customization of Work Group settings, approve individuals for membership, and upload any initial content.

The Originator must provide the following information when applying for a Secure Work Group via the on-line form (http://pbma.hq.nasa.gov/swg/):

- Name
- Title
- NASA Center affiliation
- Organization
- Work Phone
- E-mail Address
- Name of Work Group
- Summary Description of Work Group (1-2 Sentences)
- Detailed Description/Purpose of the Working Group (1-2 Paragraphs)
- Secret Question or Phrase[1]
- Response to Question or Phrase

Since passwords will only be issued verbally, the secret question or phrase and response are for verification purposes.

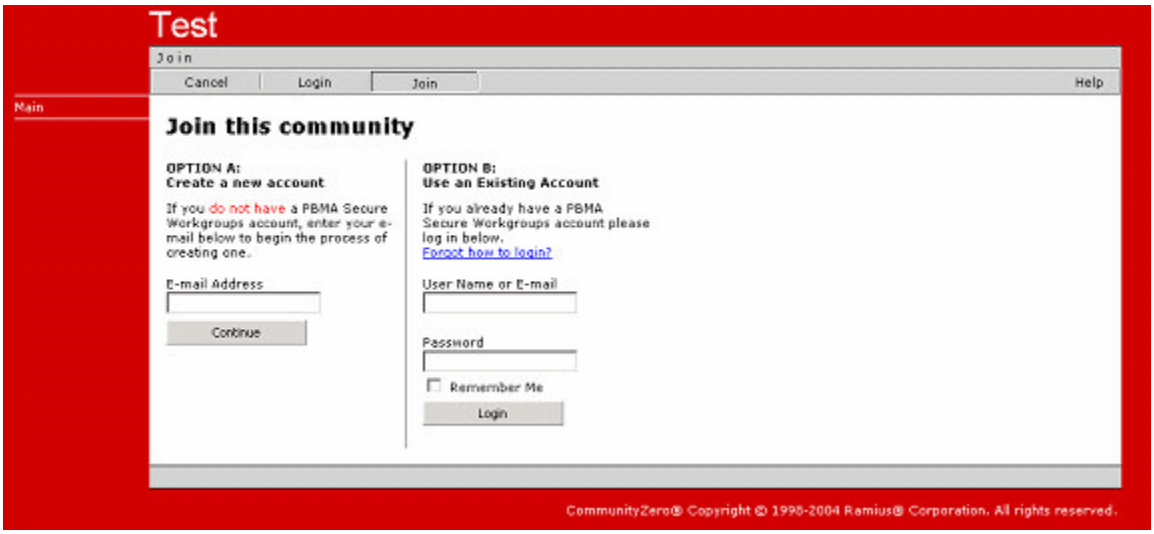
[1] A secret question or phrase is required only when requesting a Secure Work Group that will contain sensitive information, and only the first time a request is made.

3.6 Having Work Group Members Create Their Accounts

Once the Secure Work Group has been created, it has to be populated. Membership in a PBMA Secure Work Group requires approval by the Originator or a designated Administrator for every user. Once a potential Member has been deemed eligible and the "need to know" has been established to have access to the Work Group and the inherent data, the Originator/Administrator must send each member the Work Group URL and have them create their account.

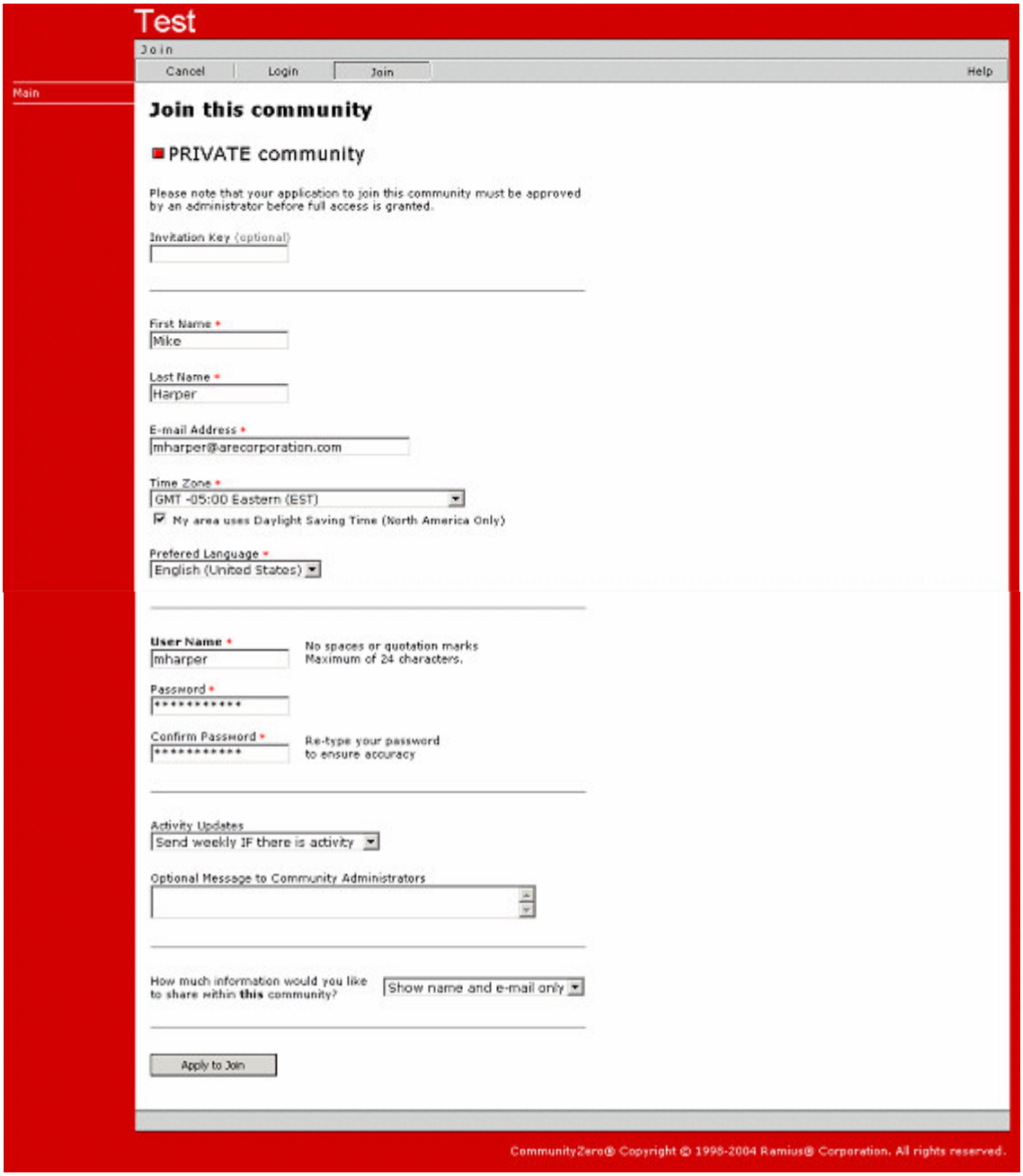
The following steps outline the process for creating a member account:

1. Once the Originator or Administrator sends the secure work group URL to the member that is to join, he/she must open the secure work group site in their Web browser.
2. Click the "Join" option at the top of the page.
3. If you are not a member of any secure work group, then choose "OPTION A: Create a new account" by typing in a valid email address and then clicking the "Continue" button.



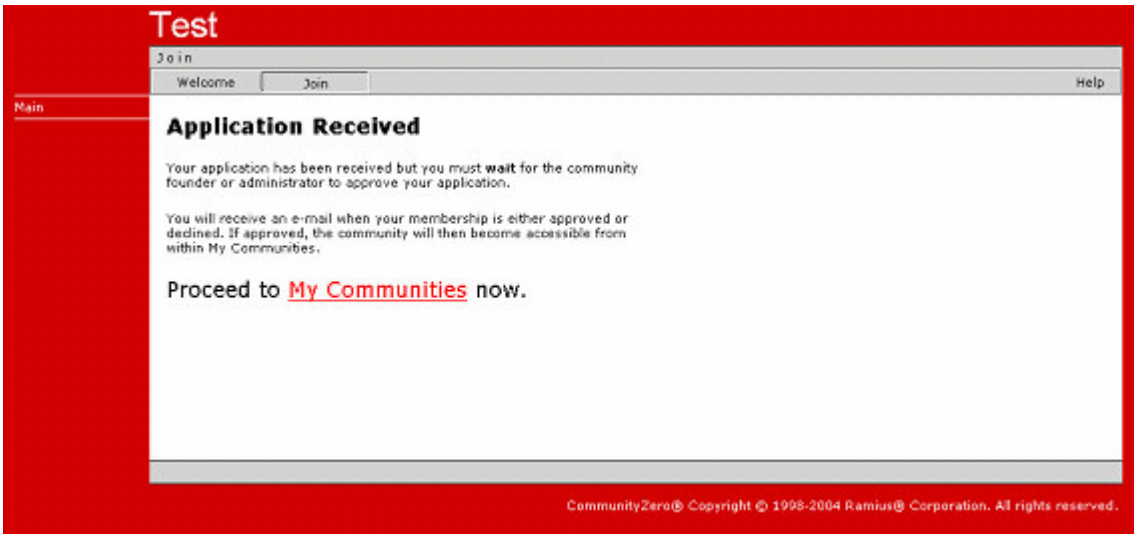
Note: If you are already member of a Work Group, then you have an existing secure work group account. Therefore choose "OPTION B: Use an Existing Account" by filling out your login information and clicking the "Login" button. On the next page, simply click "Apply to Join"

4. Fill out the following setup information and click “Apply to Join”

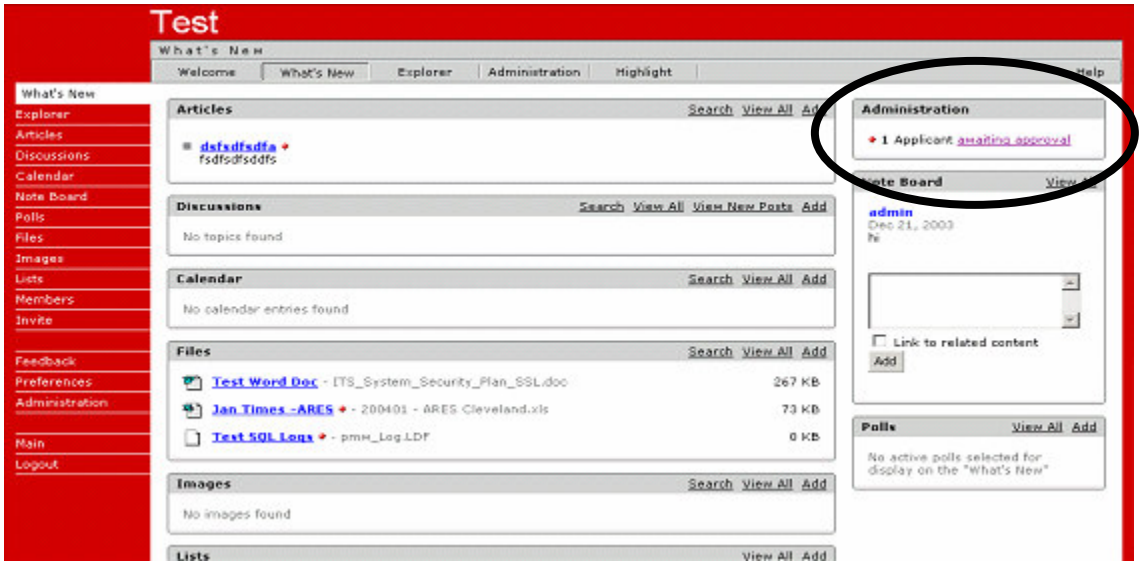


Note: Only those fields with red asterisks are needed to complete this step in the process.

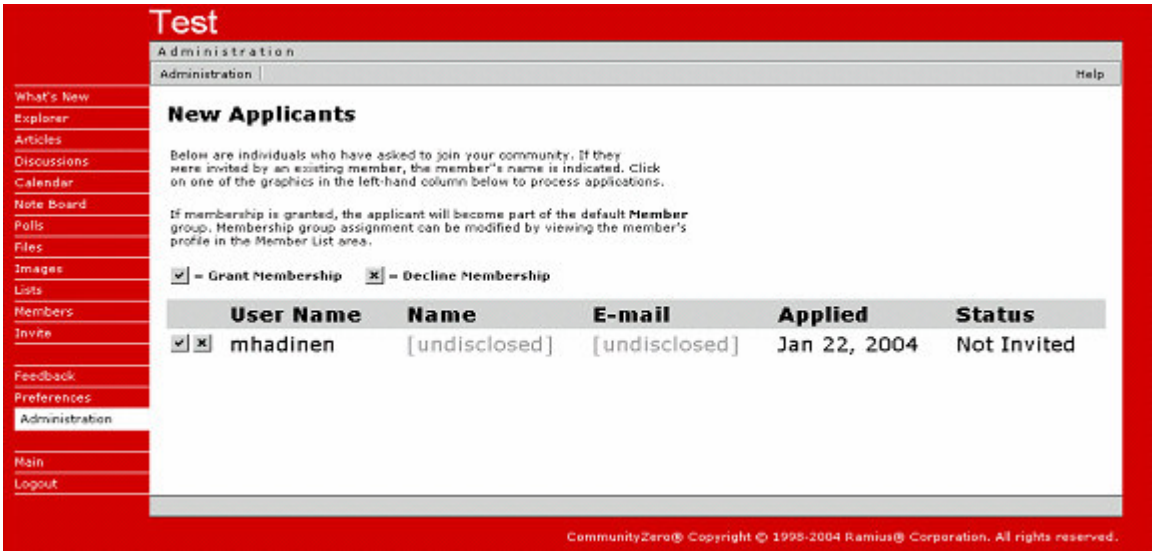
5. The member has now completed their membership profile. The application has been sent and the member must await approval from either the Originator or one of the Administrators.



6. The Originator or one of the Work Group Administrators must log into the secure work group. On the "What's New" page in the **Administration** section (shown below), the Originator or Administrator must click the "awaiting approval" link.



7. The Secure Work Group Originator or Administrator has the ability to either **Grant Membership** or **Decline Membership** on this page.

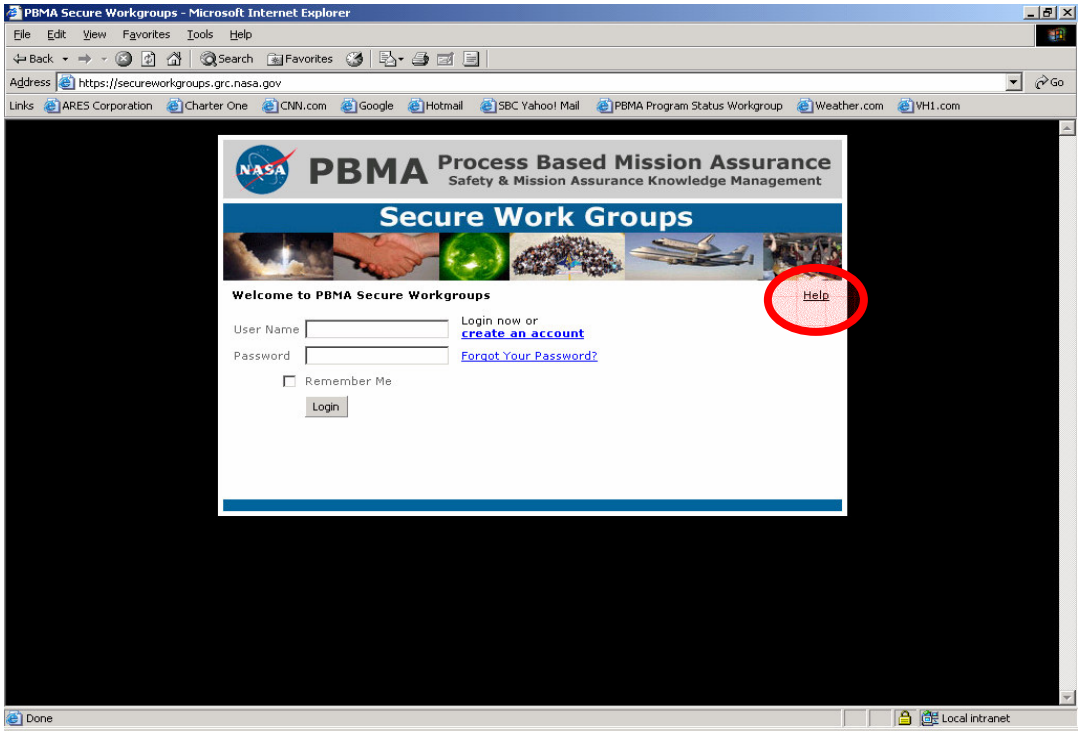


8. The new member will receive an email once the Originator or Administrator has granted membership.
9. The new member may then proceed to the Work Group site and login.

The member profile created in the initial process is that user's permanent PBMA Secure Work Groups profile. This application takes advantage of secure single sign-on (SSO). **This means that a user can keep the same user name and password for all future SSL Work Groups.** If a user creates different accounts, it will defeat the purpose of SSO. Once a user's profile is created, he/she can login at **https://secureworkgroups.grc.nasa.gov/** and all SSL Work Groups that individual belongs to will be listed. The user can then move securely to and from each Work Group available to them without having to login again.

4 GETTING HELP

Technical Support is available when the information provided in this document and online help proves insufficient. All support issues will be routed to the Help Desk via the "Help" link found at https://secureworkgroups.grc.nasa.gov/ as seen below.



As an example, the responsibility of managing password resets and reissues will belong to Technical Support. If a user needs their password reset, they must choose the "Reset Password" option from the scroll down menu. Once the user submits their request to the Help Desk, Technical Support will create a new random password and provide it to the Originator.

Note: The Originator has the responsibility to communicate password changes to their members.

Information to have available when PBMA-SSL Technical Support contacts you:

- Name
- Work Group
- Response to Secret Question

Technical support can only be contacted via the Help link. All requests will be handled as quickly as possible to maintain optimal operation of the Work Groups. Any requests

received outside of standard operating hours will be handled as soon as possible the following business day.

5 PROCESS FOR INCREASING DISK STORAGE SPACE

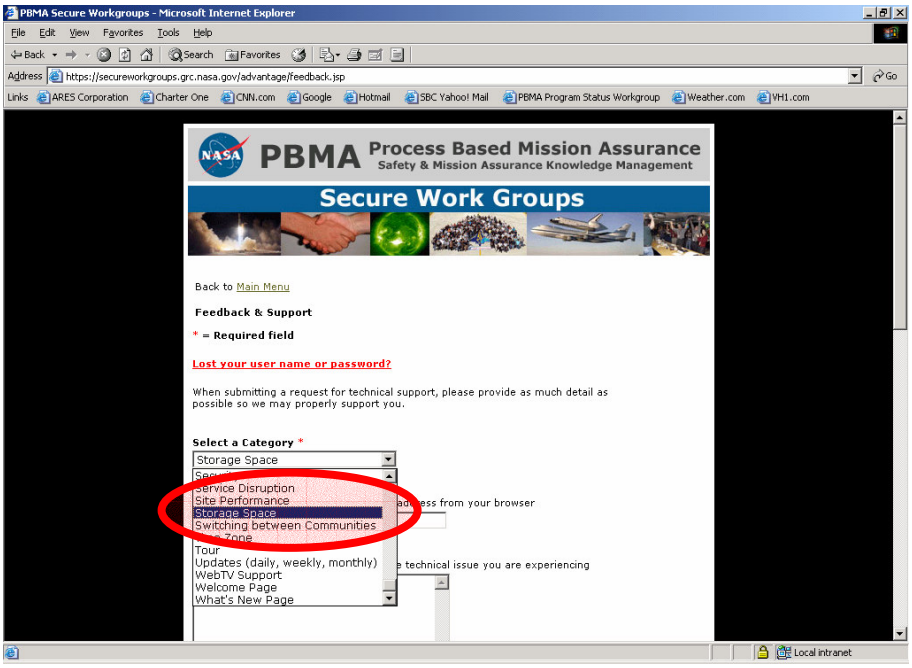
5.1 Requesting Additional Disk Storage Space

5.1.1 Approvals Required

Any Originator or Administrator may request an increase in the storage capacity of a Work Group for which they have responsibility.

5.1.2 Submitting the Request

When requesting additional storage capacity, go to the Help link and submit request to the Help Desk as seen below.



Requests are often processed on the day that they are received; however, you should allow five (5) business days.

6 PROCESS FOR DISCONTINUING A WORK GROUP

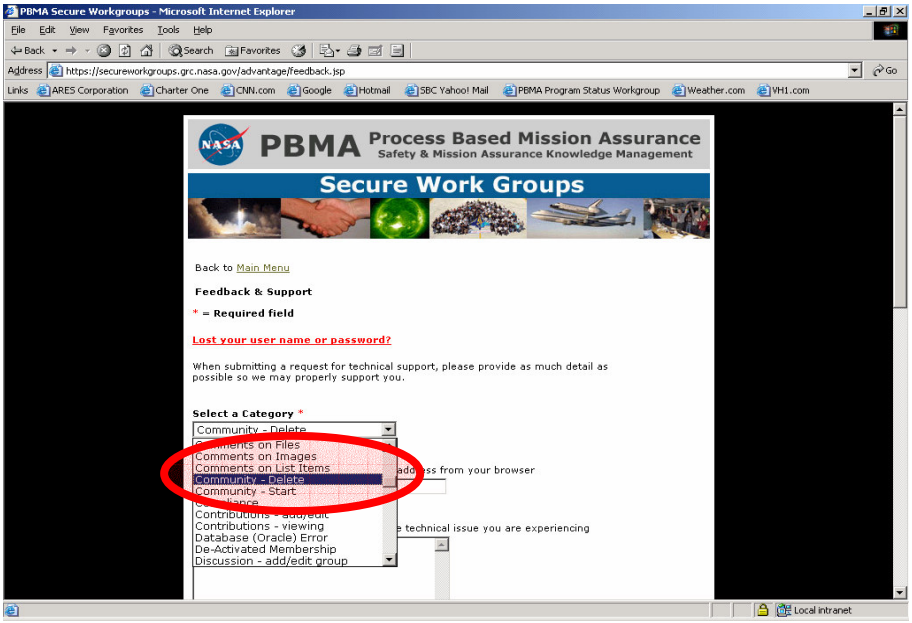
If a Work Group is no longer necessary, the Work Group must be deleted. Requesting deletion of a Work Group is the responsibility of the Originator.

6.1 Notify Members of Pending Deactivation

An Administrator of the Work Group must notify all Members that the site will be deleted. This can be accomplished by posting an announcement on the Work Group site itself, by sending an e-mail to the entire membership, or both. The message should include the expected deletion date and a reminder to Members that any data stored on the site will become unavailable following deletion.

6.2 Submitting the Request

The request to discontinue a Work Group must be submitted using the Help link and submit request to the Help Desk as seen below.



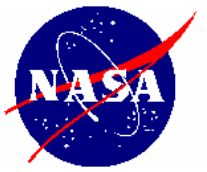
Requests are often processed on the day that they are received; however, you should allow five (5) business days.

7 TECHNICAL SUPPORT INFORMATION

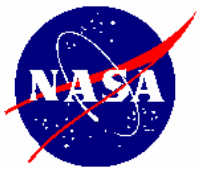
Contacting Technical Support should be made using email and addressed to pbma_workgroup@arescorporation.com

Standard operating hours of Technical Support are Monday through Friday 8:00 AM to 5:00 PM EST. Technical Support will observe all NASA holidays.

8 PBMA SECURE WORK GROUPS CHARTER



NASA Process Based Mission Assurance
Secure Work Groups (PBMA-SSL)
General Charter



Secure Work Groups are available as an enhanced functionality of Process Based Mission Assurance (PBMA). These Secure Work Groups provide multi-dimensional, collaborative functionality to support the NASA Safety and Mission Assurance community, individual program/project teams as well as formal and informal groups of subject matter experts.

Secure Work Groups for Sensitive Data

Membership is limited to those individuals involved in making NASA programs and projects successful, including contractors, industry partners, and academia. Membership in the community is predicated on the notion of reciprocity and sharing of knowledge as well as responsiveness to the needs and inquiries of the community.

Legal/Security Ground Rules

- No classified information.
- Work Group Members must be verified by their Work Group Originator.

Secure Work Groups for Non-Sensitive Data

Secure Work Groups are available for those groups that do not have a need to handle sensitive information. These Work Groups **DO NOT** have authorization to share ITAR/EAR, SEB, or other sensitive information that falls under the classification of ACI.

These Work Groups have the same functionality as those that handle ACI and can be used for that purpose once the Work Group Originator has completed the process (http://pbma.hq.nasa.gov/swg/activation_process.htm) of signing the PBMA-SSL IT Security Plan and submitting the NAC Verification Form.

Legal/Security Ground Rules

- No classified information.
- No material protected under Federal Export Control and International Traffic in Arms Regulations.
- No competition sensitive or proprietary information.
- No other sensitive material within the ACI category.

For additional information on these topics please contact your center Export Administrator or Export Counsel listed at:
http://www.hq.nasa.gov/office/codei/nasaecp/

Or access the following NASA documents:

- OMB Circular A-130
- NPR 2190.1: NASA Export Control Program
- NPD 2110.1: Foreign Access to NASA Technology Utilization Material
- NPD/NPG 2800.1: Managing Information Technology
- NPD/NPG 2810.1: Security of Information Technology
- NPG 1620: Security Procedures and Guidelines
- NIST 800-53: Recommended Security Controls for Federal Information Systems

Work Group Originator Requirements

- Review information content of the community space to assure the Work Group is not violating NASA policies regarding information security and technology transfer
- Manage and control Work Group membership and access
- Notify new members that join the Work Group outlining their responsibilities
- Prepare concise Work Group statement of purpose (two or three sentences)
- Prepare Work Group charter (two or three paragraphs)
- Visit community space on a regular basis and add new information, update or remove old information
- Mentor new members in the general functioning of the specific community

Work Group Member Requirements

- Activities that will not be tolerated and are grounds for termination of participation include:
    - Using the community space for unprofessional means, i.e., spamming, flaming, etc.
    - Violating the NASA policies regarding information disclosure
    - Violating the NASA policies regarding security and personnel safety
- Review the community-specific charter and pertinent literature including postings to the community space
- Biographical sketch for posting in the community space

Work Group Support Activity

- Periodic workshops will be conducted providing lessons learned and best practice case studies for Work Group Originators
- General metrics such as number of members, last date of activity within a Work Group, etc., will be collected and reported to PBMA management

Appendix A – National Agency Check Verification

NAC Verification Form for PBMA-SSL Work Groups

PLEASE write legibly and read thoroughly.

All Secure Work Groups that contain ACI data require that you must have the approval signature of your appropriate Center's security personnel. Requests should be delivered to PBMA-SSL Technical Support, c/o ARES Corporation, 21000 BrookPark Rd., MS 501-4, Cleveland, OH 44135, or Fax to 1-216-433-2701.

Name _____ Title _____

Center _____ Work Phone _____

Organization _____ E-mail Address _____

You are requesting access to a Secure Work Group that will be approved for sensitive but unclassified data.

You agree that unauthorized use of the computer accounts and computer resources to which you are granted access may be a violation of NPG 2810.1 and NPR 2190.1. You will make every effort to protect your account(s) from unauthorized access and will not knowingly permit access by others. Misuse of your assigned account and by accessing others' accounts without authorization is not allowed. You understand that these resources are subject to monitoring and recording by the Glenn Research Center to detect unauthorized use in accordance with NPG 2810.1. You further understand that failure to abide by these provisions may constitute grounds for termination of account access, administrative action, and/or civil or criminal liability as set forth in NPG 2810.1, NPR 2190.1, NPG 1620.1 and other applicable laws and regulations.

All users must follow these additional rules:

- NO Classified Information may be posted in these work groups
- Protect data as outlined in Section 2 of the PBMA-SSL New User Authentication And Activation Plan (NUAAP)
- Secure Work Groups are to be used for official NASA business ONLY.

I certify that I am a United States citizen and have had a National Agency Check (NAC) performed.

I, _____ hereby certify that I understand, and upon the granting of access to the Web server shall comply with all above statements.

_____ _____
Work Group Originator Signature Date

_____ _____ _____
Center Security Representative Signature Phone Number Date

For Internal Use Only

_____ _____
Verification of Citizenship and NAC by Technical Support **Date**